



# Department of Homeland Security Daily Open Source Infrastructure Report for 30 June 2006

Current  
Nationwide  
Threat Level is



[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Federal Bureau of Investigation in Baltimore, Maryland, has announced the recovery of the stolen Veterans Administration laptop computer and external hard drive taken during a burglary on Wednesday, May 3. (See item [12](#))
- The Department of Homeland Security is providing personnel and assets from two key operational component agencies, the Federal Emergency Management Agency and the United States Coast Guard, in support of state and local response efforts to ongoing flooding in the Mid-Atlantic region. (See item [32](#))
- The Associated Press reports Cecil County, Maryland, officials have asked residents of low-lying areas around the Conowingo Dam to evacuate Thursday, June 29, before the Susquehanna River reaches peak flow causing flooding. (See item [40](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 30, News-Sentinel (IN)* — **Area soy-powered station is a first.** Residents and businesses in the growing Lafayette Township area will soon get their power from a substation using the state's first soybean-oil-powered transformer. United REMC, an electric provider,

will showcase the new substation on Lafayette Center Road near North Gundy Road to the public. The transformer will use environmentally safe FR3 soybean oil produced by Wisconsin-based Cooper Power Systems, instead of petroleum-based and environmentally toxic mineral oil. The substation will begin service in July, said John Klingenger, United REMC's corporate relations manager, and immediately send power to about 1,800 customers currently served by the old substation. FR3 fluid is made from edible vegetable oils and additives, and contains no petroleum, halogens or silicones. It is produced in the U.S. using soybeans from American farmers. Allen County Extension Agent Gonzalee Martin said, "I would be surprised if it did not become the industry norm."

Source: <http://www.fortwayne.com/mld/newssentinel/business/14929396.htm>

2. *June 29, Associated Press* — **Oil pipeline ruptures near Little Falls, Minnesota.** Pollution control officials estimate that 67,000 gallons of oil spilled after a crude oil pipeline ruptured near Little Falls, MN. Cleanup crews were on the scene Wednesday, June 28, trying to recover oil from the leak that was spotted Tuesday night. Steve Mikkelsen of the Minnesota Pollution Control Agency says it's not clear yet what caused the break in the 16-inch pipeline. Firefighters and deputies were able to shut down the leak. State pipeline safety and pollution control officials determined there was no immediate risk to public safety, and no evacuation was necessary.

Source: <http://www.winonadailynews.com/articles/2006/06/28/mn/oil.txt>

3. *June 29, San Francisco Chronicle* — **Weapons labs hit for poor oversight of their explosives.** Tons of chemical explosives are improperly monitored at two nuclear weapons laboratories in New Mexico and, as a result, may be at risk of theft, according to a federal audit released this week. The explosives may also be unsafe because neither of the labs — Los Alamos and Sandia national laboratories — routinely checks their "stability and safety characteristics," the U.S. Energy Department's inspector general said in the report. During a federal inspection, Sandia officials "could not account for at least 410 items, including detonators, rocket motors, shaped explosives and bulk explosive powders," the report said. In addition, that lab's inventory system lacked records for about 190,000 pounds of explosive propellant used in 39 rocket motors. The report said Los Alamos has "accumulated significant amounts of high explosive materials that were unlikely to be used for current or future missions."

Report: <http://www.ig.doe.gov/pdf/IG-0730.pdf>

Source: <http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/06/29/MNGICJM9B41.DTL>

4. *June 28, Associated Press* — **FirstEnergy hopes \$22 million control center improves reliability.** Behind barbed wire at a secret location, FirstEnergy Corp. hopes a \$22 million control center improves electric reliability for customers. FirstEnergy's Robert Austin said the new equipment allows the utility to check monitors at 42,000 locations on high-voltage lines and big substations every five minutes. The upgraded control center completed June 1 and its eastern Pennsylvania twin are linked by phone and computer to regional grid operators, giving FirstEnergy the ability to know when a big power line fails hundreds of miles away and the effect on the system here. The bombproof center's 35 dispatchers today are backed up by hundreds of engineers. The centerpiece of FirstEnergy's center is a 70-foot by 7-foot video screen that can have one huge picture or as many as 700. If a transmission line goes down, that information flashes on a computer screen in seconds and an engineer can open and close

switches to minimize the damage. American Electric Power is spending \$44 million to build a similar facility in central Ohio.

Source: <http://www.dfw.com/mld/dfw/business/14923537.htm>

5. *June 28, Radio New Zealand* — **Transpower checks 170 substations nationwide.** Transpower has started nationwide inspections of substation equipment following a major power outage in Auckland on June 12, in which an estimated 700,000 people were affected. Some estimate the cost of the outage to be as high as \$50 million. A report released on Tuesday, June 27, blamed the blackout on high winds causing two rusted D-shackles to break at the Otahuhu substation. Transpower's maintenance records and schedules were found to be adequate at the substation, but the report said the poor condition of the shackles should have been picked up during checks in 2003. Transpower spokesperson Chris Roberts says checks will be made on all 170 substations around the country by the end of July. Energy Minister, David Parker, says investigations are being conducted into how to diversify supply into Auckland.

Source: <http://www.radionz.co.nz/news/latest/200606281957/286601d>

6. *June 28, 1010 News (NY)* — **Not all sirens perform in Indian Point test.** Almost all the emergency sirens around the Indian Point nuclear power plants sounded during a test Wednesday, June 28, a major improvement over the results three months ago. At least 144 of the 156 sirens, which are meant to alert residents within a 10-mile radius to an emergency at the plants in Buchanan, sounded and rotated properly, emergency officials said. Jim Streets, spokesperson for Entergy Nuclear Northeast, owner of Indian Point, said 151 of the sirens worked but some sensors failed to relay that information to monitors. Either way, it was better than a March 8 test that locked up the siren system for hours. Streets said three sirens failed in Westchester County, one in Rockland and one in Orange County; all the sirens in Putnam County worked, he said. The Nuclear Regulatory Commission has demanded, and Entergy has promised, a state-of-the-art system by next January.

Source: <http://1010wins.com/pages/51211.php?>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

7. *June 29, Associated Press* — **One hurt in house explosion; chemical in sewer system suspected.** A house explosion in Quincy, MA, left one man injured Wednesday night, June 28. Deputy Fire Chief Joe Barron said natural gas was not the culprit because there was no gas line running to the property. Officials suspect the explosion was caused by a highly-flammable solvent that had been flushed into the sewer system.

Source: [http://www.boston.com/news/local/massachusetts/articles/2006/06/29/one\\_hurt\\_in\\_house\\_explosion\\_chemical\\_in\\_sewer\\_system\\_suspected/?rss\\_id=Boston+Globe+--+City+Weekly](http://www.boston.com/news/local/massachusetts/articles/2006/06/29/one_hurt_in_house_explosion_chemical_in_sewer_system_suspected/?rss_id=Boston+Globe+--+City+Weekly)

8. *June 29, Oklahoman* — **Chemical spill prompts evacuation, road closure in Oklahoma.** Thursday, June 29, Hazmat crews were on the scene of an overturned 18-wheel flatbed on U.S. 270 near Calvin in Hughes County, OK. The truck was carrying pods with at least four chemicals and some leaked. At least one chemical emitted a cloud to the south, causing some

residents to evacuate their homes. The accident caused the shutdown of an off-ramp at U.S. 270 and U.S. 75.

Source: <http://www.newsok.com/article/1880922>

9. *June 29, Associated Press* — **Two trucks land in Lochsa River, spilling diesel.** A pair of semi-trucks nearly collided and both landed in the Lochsa River in the rugged U.S. Highway 12 corridor in north-central Idaho yesterday afternoon, Wednesday, June 28. Idaho State Police officials say one of the trucks spilled about 200 gallons of diesel fuel into the water.

Source: [http://www.ktvb.com/news/localnews/stories/ktvbn-jun2906-trucks\\_spill.ba9e5b9.html](http://www.ktvb.com/news/localnews/stories/ktvbn-jun2906-trucks_spill.ba9e5b9.html)

[[Return to top](#)]

## **Defense Industrial Base Sector**

Nothing to report.

[[Return to top](#)]

## **Banking and Finance Sector**

10. *June 29, McClatchy Newspapers* — **Best Buy getting proactive in identity-theft battle.** Best Buy Co. Inc. is beefing up security spending by \$15.5 million this year, the first of a two-year effort to tighten computer security. The company hires pseudo-hackers to try to break into its networks before real hackers might. Best Buy describes a sweeping computer security project that touches nearly every aspect of data-handling by hundreds of computer systems. It described 50 "control points" where Best Buy has appointed "data stewards" to strictly monitor which employees can access customer credit card information. Best Buy limits how much customer information an employee can carry out of the company on a laptop, by making the downloading process laborious. Best Buy also is increasing security at the store level, from training employees not to print out a credit card application and leave it on the printer to getting credit card information quickly out of the store.

Source: <http://www.siliconvalley.com/mld/siliconvalley/14922818.htm>

11. *June 29, Washington Post* — **Identity thieves hit NIH Credit Union.** The National Institutes of Health's (NIH) federal credit union has notified some customers that their personal information has been compromised by an identity theft scheme, officials said Wednesday, June 28. Lindsay A. Alexander, chief executive of the credit union, would not disclose how many of the institution's 41,000 customers were affected, but she did say it was a small number. "They already know who they are, and we know who they are, and we're working with them," she said. The Rockville-based credit union's clients include employees of NIH, several biotech companies and hospitals such as Sibley Memorial in Northwest Washington. Alexander said the theft happened recently. She said she could not reveal what type of information was stolen or how it was stolen. Local and federal agencies are investigating. The credit union is offering them free credit reports and monitoring for a year, Alexander said.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/28/AR2006062801936.html>

12. *June 29, Federal Bureau of Investigation* — **Veterans Administration stolen laptop and external hard drive recovered.** The Veterans Administration Office of the Inspector General, the Federal Bureau of Investigation, and the Montgomery County Police Department announce the recovery of the stolen laptop computer and external hard drive taken during a burglary on Wednesday, May 3. The electronic equipment contained sensitive information concerning over 26 million veterans. A preliminary review of the equipment by computer forensic teams determined that the database remains intact and has not been accessed since it was stolen. A thorough forensic examination is underway.  
Source: [http://baltimore.fbi.gov/pressrel/2006/laptop\\_062906.htm](http://baltimore.fbi.gov/pressrel/2006/laptop_062906.htm)
13. *June 28, Reuters* — **ID theft strikes South Korean leaders.** South Korea's president and prime minister appear to have become victims of online identity theft as their names were used by others to gain access to 416 Websites requiring personal identification, including 280 pornographic sites, said Ryu Keun Chan, a member of the United Liberal Democratsa member of Parliament Wednesday, June 28. The 13-digit personal identification numbers of President Roh Moo Hyun and Prime Minister Han Myeong Sook are readily accessible on Internet search engines and have been used by numerous South Koreans, said Ryu. Identification numbers along with names form the basis of almost all aspects of South Koreans' lives, from medical insurance and subscribing to a mobile phone service to paying taxes and registering on Internet sites. "When the president and the prime minister's ID numbers are available online and their stolen ID numbers are used on Websites, it's not hard to imagine how carelessly the average person is treated," Ryu said.  
Source: [http://www.iht.com/bin/print\\_ipub.php?file=/articles/2006/06/28/news/roh.php](http://www.iht.com/bin/print_ipub.php?file=/articles/2006/06/28/news/roh.php)

[[Return to top](#)]

## **Transportation and Border Security Sector**

14. *June 29, USA TODAY* — **U.S. Interstate system marks 50 years.** With the stroke of a pen 50 years ago, June 29, President Dwight D. Eisenhower launched the interstate highway system, a giant public works project that would speed travel and the distribution of goods, make driving safer, fuel the growth of suburbs, and link far-flung regions of the nation. The Federal-Aid Highway Act Eisenhower signed called for a 41,000-mile system of freeways to be built by 1975. The interstate network is getting crowded much faster than it's being expanded, and spending to expand and modernize it must increase dramatically to reduce congestion, according to a report released on Thursday, June 29. Travel on the 46,572-mile system increased by 51 percent from 1990 to 2004 while capacity grew six percent says the report by TRIP (The Road Information Project), a Washington non-profit group that promotes transportation policies that relieve congestion and aid economic productivity. Spending on interstate repairs and improvements this year is about \$17 billion — less than the \$21 billion needed to maintain highways and bridges in their current condition and keep traffic congestion from worsening, TRIP reports. It would cost \$35 billion a year for major improvements that would significantly reduce congestion, TRIP says.  
TRIP Report: <http://www.tripnet.org/>  
Source: [http://www.usatoday.com/news/nation/2006-06-28-interstate-sy stem\\_x.htm](http://www.usatoday.com/news/nation/2006-06-28-interstate-sy stem_x.htm)

15. *June 29, Detroit Free Press* — **Michigan Airport runway to get \$64–million face–lift.** Northwestern Highway in Southfield, MI, is pot–holed, patched up, and needs new asphalt. And so do a couple of runways at Detroit Metro Airport. The Wayne County Airport Authority, which runs Metro, plans to spend \$64 million in the next two years to fix one of them. Because there are five other runways available, airport officials say the work should have little effect on flights. The airport's board is expected hire a local contractor to rebuild the runway for \$41 million. The rest of the money will go for designing the project and updating areas around the runway, including lighting, airport spokesperson Barbara Hogan said. Full funding has yet to be approved, but the Federal Aviation Administration is expected to cover about \$48 million. The airport will pay the final \$16 million by using fees airlines pay to land at Metro.  
Source: <http://www.freep.com/apps/pbcs.dll/article?AID=/20060629/BUSINESS05/606290391>
16. *June 29, Department of Homeland Security* — **U.S. borders strengthened through the Secure Border Initiative.** The Department of Homeland Security (DHS) is strengthening security along the nation's northern and southern borders through the Secure Border Initiative (SBI) and other efforts. The SBI integrates increased manpower and infrastructure, cutting–edge technology, enhanced immigration enforcement, and cooperation among state, local, and international partners to bolster border security. Through SBI, the United States is constructing new fencing and barriers and improving and expanding existing infrastructure. DHS is also using 21st century technology to increase the effectiveness of operations. The use of radiation detectors, sensors, cameras, and biometric information dramatically increases the likelihood of apprehending terrorists and other criminals attempting to enter the United States.  
Source: [http://www.dhs.gov/dhspublic/interapp/press\\_release/press\\_release\\_0938.xml](http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0938.xml)
17. *June 29, Transportation Security Administration* — **TSA says leave fireworks and lighters at home this July Fourth.** In anticipation of the Fourth of July holiday, the Transportation Security Administration (TSA) reminds travelers that fireworks — including sparklers and bottle rockets — are prohibited in checked baggage and from passing through security checkpoints. Other common prohibited items include firearms, knives, pocketknives, lighters, and box cutters. TSA security officers continue to intercept over 30,000 lighters a day nationwide, which results in delays for every passenger at the security checkpoint. Bringing prohibited items to the checkpoint can result in a fine of up to \$10,000 and possible arrest and imprisonment. “This summer will be one of busiest travel seasons on record. Passengers can help us keep wait times down at security checkpoints by leaving prohibited items such as lighters and fireworks at home,” said Kip Hawley, Assistant Secretary for TSA. This summer, TSA and other aviation partners will welcome more than 200 million air travelers to the nation's airports during the peak summer travel period between Memorial Day and Labor Day weekends. TSA is prepared to address the needs of the traveling public this summer, which is predicted to be the busiest travel season yet.  
TSA Summer Travel Tips: <http://www.tsa.gov>  
Source: [http://www.tsa.gov/public/display?theme=44&content=090005198\\_01fd395](http://www.tsa.gov/public/display?theme=44&content=090005198_01fd395)
18. *June 29, Government Accountability Office* — **GAO–06–875T: Aviation Security: TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems, but Funding Uncertainties Remain (Testimony).** The Transportation Security Administration (TSA) has deployed two types of baggage screening equipment: explosive

detection systems (EDS), which use X-rays to scan bags for explosives, and explosive trace detection systems (ETD), in which bags are swabbed to test for chemical traces of explosives. TSA considers screening with EDS to be superior to screening with ETD because EDS machines process more bags per hour and automatically detect explosives without direct human involvement. In March 2005, GAO reported that while TSA had made progress in deploying EDS and ETD machines, it had not conducted a systematic, prospective analysis of the optimal deployment of these machines to achieve long-term savings and enhanced efficiencies and security. GAO's testimony today updates our previous report and discusses TSA's (1) deployment of EDS and ETD systems and the identified benefits of in-line systems, and (2) planning for the optimal deployment of checked baggage screening systems and efforts to identify funding and financing options. The Government Accountability Office previously recommended that TSA systematically evaluate checked baggage screening needs at airports, such as identifying the costs and benefits of installing in-line systems or stand-alone EDS. DHS generally concurred with our recommendations.

Highlights: <http://www.gao.gov/highlights/d06875thigh.pdf> Source:

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-875T>

19. *June 29, Associated Press* — **Hawaiian Air seeks to ground Mesa Air.** Hawaiian Airlines on Wednesday, June 28, filed a motion seeking a court order to prevent Mesa Air Group Inc. from issuing interisland tickets for a year, alleging the new interisland carrier illegally used confidential information. Hawaiian said it has proof Mesa and its chief financial officer, George Murnane III, misled the U.S. Bankruptcy Court about the use of "highly confidential" documents and trade secrets obtained from Hawaiian in April 2004. Mark Dunkerley, Hawaiian's president and chief executive, said in a statement that Hawaiian is seeking remedy for Mesa breaching a confidentiality agreement. Mesa on June 9, launched go! airlines as the third interisland jet carrier in Hawaii, entering the exclusive market dominated for decades by Hawaiian and Aloha airlines and sparking an airfare war.

Source: [http://biz.yahoo.com/ap/060629/hawaii\\_air\\_war.html?v=1](http://biz.yahoo.com/ap/060629/hawaii_air_war.html?v=1)

20. *June 29, Reuters* — **Toronto island airline to press on, shuns protests.** A new airline set to start operating out of Toronto's city center island airport later this year announced its first route Tuesday, June 27, dismissing protests from opponents who say the carrier will cause excessive noise and should be denied permission to fly. Porter Airlines President Robert Deluce said service would begin with 10 round trips a day to Ottawa from the island, which is close to Toronto's downtown financial hub. The carrier — which has ordered ten 70-seat turboprop planes from Bombardier Inc. and has options for another 10 — eventually plans to fly to 17 cities in the United States and Canada, including Boston, Chicago, Washington, New York, Philadelphia, Detroit, and Montreal. The only link to the airport is a small ferry service. The Toronto Port Authority is promising a new updated ferry, which Deluce said would allay his earlier concerns about the need for better access to the airport.

Source: [http://www.usatoday.com/travel/flights/2006-06-28-porter-air\\_x.htm](http://www.usatoday.com/travel/flights/2006-06-28-porter-air_x.htm)

[[Return to top](#)]

## **Postal and Shipping Sector**

21.

*June 28, Memphis Business Journal (TN)* — **UPS, USPS sign air transportation deal.** United Parcel Service Inc. (UPS) has signed a three-year deal with the U.S. Postal Service (USPS) to provide domestic air transportation of primarily First Class and Priority Mail starting July 1. Atlanta-based UPS at first will provide airlift of First Class and Priority Mail volume each week to and from 98 cities, it said. The contract, which includes an option for one two-year extension, expands an existing relationship between UPS and the USPS, under which the company provides airlift for mail transportation between 16 cities.

Source: <http://biz.yahoo.com/bizj/060628/1307968.html?.v=2>

[\[Return to top\]](#)

## **Agriculture Sector**

**22. *June 29, Animal and Plant Health Inspection Service* — Final rule regarding Idaho's brucellosis status adopted.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is finalizing, without change, an interim rule amending its brucellosis regulations concerning interstate movement of cattle by changing Idaho's classification status from Class Free to Class A. This is a necessary action in order to prevent the spread of brucellosis. Brucellosis Class-Free status is based on a state carrying out all requirements of the brucellosis program and finding no cases of brucellosis in cattle and bison for 12 months. APHIS has determined that Idaho no longer meets the standards for Class-Free status. Idaho was classified as Class Free until a brucellosis infected herd was discovered on November 14, 2005. At that time, the state took immediate measures to maintain its Class-Free status according to federal regulations. However, on November 29, 2005, another brucellosis infected herd was confirmed. With the discovery of the second infected herd, Idaho no longer meets the standards for Class-Free Status. Brucellosis is a contagious disease caused by the brucella bacteria, and affects animals. Aside from Idaho, only two other states are affected with cattle brucellosis, Wyoming and Texas.

Source: <http://www.aphis.usda.gov/newsroom/content/2006/06/idahobru.shtml>

**23. *June 29, U.S. Department of Agriculture* — Emergency conservation program funding for 18 states announced.** U.S. Department of Agriculture (USDA) Deputy Secretary Chuck Conner Thursday, June 29, announced that USDA will begin allocating \$11.8 million in Emergency Conservation Program (ECP) funding for 18 states to help producers rehabilitate land damaged by natural disasters. ECP gives producers additional resources to remove debris from farmland, restore fences and conservation structures, provide water for livestock in drought situations and grade and shape farmland damaged by a natural disaster. Eligible producers will receive cost-share assistance of up to 75 percent of the cost of the approved practice.

Source: [http://www.usda.gov/wps/portal/!ut/p/s.7\\_0\\_A/7\\_0\\_1OB?contentidonly=true&contentid=2006/06/0227.xml](http://www.usda.gov/wps/portal/!ut/p/s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/06/0227.xml)

**24. *June 28, AgProfessional* — Traps placed to track Western Bean Cutworm.** Pioneer Hi-Bred International Inc. has joined the effort to track the eastward movement of western bean cutworm (WBC), a destructive pest that can reduce corn yields by as much as 30 percent to 40 percent. Pioneer agronomists and sales representatives in Iowa, Illinois, Missouri, Minnesota and Wisconsin will place and monitor more than 200 WBC pheromone traps. Extension

entomologists at Iowa State University, University of Missouri, University of Wisconsin, Purdue University and the University of Illinois also will be tracking the movement of this insect.

WBC Monitoring Network: <http://www.ent.iastate.edu/trap/westernbeancutworm/>

Source: [http://www.agprofessional.com/show\\_story.php?id=41468](http://www.agprofessional.com/show_story.php?id=41468)

25. *June 28, Associated Press* — **New rule to attempt to cut herd in chronic wasting disease zones.** The Wisconsin Department of Natural Resources wants to have a shorter gun deer hunting season in chronic wasting disease (CWD) zones and allow hunters to shoot as many deer as they like there. Under a new rule being considered by a state Senate committee, hunters would no longer have to "earn a buck" by shooting a doe. The rationale behind the new rules is that hunters want a shorter season with simpler rules. Since the fatal brain disease was discovered in the wild white-tailed deer population in 2002, the state has spent close to \$30 million to fight the disease, but there has been no significant herd reduction.

CWD information: <http://www.cwd-info.org/>

Source: <http://www.duluthsuperior.com/mld/duluthsuperior/news/politics/14922717.htm>

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

26. *June 29, Computing* — **Utility to introduce satellite tracking.** Severn Trent Water is to install satellite tracking technology in its 1,000-strong fleet of vehicles to tighten security and improve monitoring. The utility, which supplies water to eight million people in the United Kingdom, has been piloting tracking technology in 20 vehicles, and now wants to extend it to the whole fleet. Severn Trent transport manager Gerald Pollard says the pilot project was only meant to cover issues such as the protection of lone workers and locating stolen vehicles, but generated other benefits including traffic monitoring and the ability to pinpoint employee locations.

Source: <http://www.computing.co.uk/computing/news/2159352/utility-introduce-satellite>

27. *June 28, Call (RI)* — **Two sentenced for tank tampering.** One of two boys who broke into a Bellingham Road water tank, in Blackstone, RI, earlier this year in a security breach was ordered to enter a residential facility for emotionally troubled teens. The boys, both 15, appeared for sentencing recently in Milford Juvenile Court on charges related to the break. Each of the two boys was ordered to pay \$6,000 in damages and serve 200 hours of community service. The boys were arrested on March 27 after police and public works officials investigated a malfunction report on a computer monitoring a 1.3 million-gallon water tank on Bellingham Road. After scaling a barbed wire fence, the boys climbed onto the tank, pried open a vent and urinated in the tank, according to police and other officials. Because a container with a chemical odor was found near the tank, investigators were uncertain whether the youths had

poured potentially harmful substances into the water, prompting health officials to ban the use of water in two states. The order affected more than 7,000 residents.

Source: [http://www.zwire.com/site/news.cfm?newsid=16855604&BRD=1712&PAG=461&dept\\_id=24361&rft=6](http://www.zwire.com/site/news.cfm?newsid=16855604&BRD=1712&PAG=461&dept_id=24361&rft=6)

[\[Return to top\]](#)

## **Public Health Sector**

28. *June 29, Agence France–Presse* — **Bird flu conference warns of gaps in knowledge, preparedness.** A major conference on avian flu, convened amidst a rising death toll among humans and a widening geographical spread among birds, warned of weak defenses and worrying gaps in knowledge about the lethal virus. Experts at the start of the two–day Paris, France, meeting cautioned there remain too many holes in basic understanding how the virus is transmitted by wild birds, whether it could be carried by other animals and how it could one day become contagious among humans. At the same time, illegal trade in poultry is flourishing and veterinary surveillance in parts of Asia and Africa is sketchy at best, providing plenty of opportunities for the disease to spread undetected among flocks and leap to humans, they said. Source: <http://www.todayonline.com/articles/127638.asp>

29. *June 29, Xinhua (China)* — **China strengthens surveillance of flu–like outbreaks.** China's Ministry of Health on Wednesday, June 28, issued guidelines for reporting and investigating flu–like cases to strengthen surveillance of possible outbreaks. China has seen a number of influenza–like outbreaks in recent years and the outbreaks usually occur at places where a lot of people are clustered together such as schools. The guidelines require that places with more than 30 flu–like cases in a week, or five cases of hospitalization, or one fatality caused by these diseases should report to the county's center for disease control and prevention (CDC) within two hours after the discovery. Once lab tests confirm the cases as influenza, information of every individual case should be reported directly to the ministry through the network. Source: [http://english.people.com.cn/200606/29/eng20060629\\_278333.ht ml](http://english.people.com.cn/200606/29/eng20060629_278333.ht ml)

[\[Return to top\]](#)

## **Government Sector**

30. *June 29, Associated Press* — **IRS closed for a month to repair flood damage.** The Internal Revenue Service (IRS) headquarters in Washington, DC, will remain closed for at least a month to repair extensive flood damage that destroyed electrical systems and computer equipment. The agency says the closure will not affect IRS service or tax enforcement because its operations are spread around the country. This week's heavy rains left 20 feet of water in the building's sub–basement. Almost all the building's electrical and maintenance systems are damaged or destroyed. The flooding also damaged offices, furniture, computer equipment, and vehicles. Source: [http://www.wusatv9.com/news/news\\_article.aspx?storyid=50462](http://www.wusatv9.com/news/news_article.aspx?storyid=50462)

[\[Return to top\]](#)

## **Emergency Services Sector**

**31. *June 29, U.S. Department of Defense* — Army conducts hurricane response exercise.**

Incorporating the lessons learned from last year's devastating hurricane season, the Army held a hurricane response exercise in Fort Belvoir, VA, Wednesday, June 28. "We're practicing and rehearsing what task each command would have to execute as they go through their operational mission," said Army Col. Kenneth Madden. Participants included various Army commands, the National Guard Bureau, U.S. Northern Command, the Joint Director of Military Support and the Defense Logistics Agency. A Federal Emergency Management Agency representative also was present. "Basically, we are working to simplify the process so that we can streamline some of our efforts differently than pre-Hurricane Katrina," said Edwin Murphy, a Defense Logistics Agency action officer. The exercise highlighted where Army resources, such as personnel and equipment, are located and how to coordinate these resources to better respond to a hurricane.

Source: [http://www.defenselink.mil/news/Jun2006/20060629\\_5541.html](http://www.defenselink.mil/news/Jun2006/20060629_5541.html)

**32. *June 28, Department of Homeland Security* — DHS Responds to Mid-Atlantic flooding.** The Department of Homeland Security (DHS) is providing personnel and assets from two key operational component agencies, the Federal Emergency Management Agency (FEMA) and the United States Coast Guard, in support to state and local response efforts to ongoing flooding in the Mid-Atlantic region. FEMA has activated the Regional Response Coordination Center in Philadelphia to integrate federal support for state and local response efforts. FEMA is in contact with state emergency management officials in the impacted states and it is deploying liaisons to state Emergency Operations Centers in Maryland, Delaware, New Jersey, Pennsylvania, and the District of Columbia, to provide assistance to state officials as requested. The United States Coast Guard has two Jayhawk helicopter rescue crews conducting ongoing search and rescue operations.

Source: <http://www.dhs.gov/dhspublic/display?content=5707>

**33. *June 28, Suffolk Life (NY)* — Meeting held to plan for natural disasters in New York.** In order to avoid a tragedy like that of Hurricane Katrina, Congressman Steve Israel (NY-D) called upon senior emergency officials from the federal government to meet with local and county officials, first responders and other community leaders to establish a plan before disaster hits. Topics discussed included the development of a seamless communication system among all levels of government, methods of evacuation for families and their pets, and a plan to coordinate efforts of local hospitals and emergency first responders. According to Israel, one of the major problems with Katrina was that the federal government was unaware of who was in charge of hurricane preparedness at the local level. A great challenge on Long Island, Israel noted, is that there are so many levels of government. Huntington Town Supervisor Frank Petrone and Bay Shore Fire Chief Robert Hulse were recently selected by Israel to chair a Hurricane Preparedness Survey Working Group. The group intends to meet several times between now and September in order to close any gaps in the line of communication and hurricane preparedness.

Source: [http://www.zwire.com/site/news.cfm?newsid=16857235&BRD=1776&PAG=461&dept\\_id=6365&rfti=6](http://www.zwire.com/site/news.cfm?newsid=16857235&BRD=1776&PAG=461&dept_id=6365&rfti=6)

**34.**

*June 28, South Florida Sun–Sentinel* — **Florida city takes hurricane precautions with extra generators, training.** Weston, FL, is preparing just in case another hurricane strikes. Among the enhancements are new generators for traffic signals. The city has purchased 34 generators, one for each intersection, to operate traffic signals during a power outage. After the storm, Public Works staffers would place the generators inside cabinets that will be permanently installed next to the intersection's existing traffic controller. In May, the city started an almost \$140,000 project reconfiguring its traffic signal heads from vertical to horizontal, to better withstand high winds and flying projectiles. The city also is updating its emergency management plan to meet federal standards. Additionally, the city plans to purchase a satellite television for use at Weston's emergency operations center.

Source: <http://www.sun-sentinel.com/news/local/broward/sfl-we28prepa-rejun28.0.130342.story?coll=sfl-news-browardcomm>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

35. *June 28, Security Focus* — **U.S. Government mandates laptop security.** The Bush Administration is giving federal civilian agencies just 45 days to comply with new recommendations for laptop encryption and two-factor authentication. The memo follows a wave of high profile data thefts and major security breeches involving remote access or the theft of government laptop computers containing sensitive personal information. The official memo from the executive office of the U.S. President stipulates that all mobile devices containing sensitive information must have their data encrypted. The recommendations also say that two-factor authentication must be used for remote access, that remote access must time out after 30 minutes of inactivity, and that all data extracts must be logged.

Source: <http://www.securityfocus.com/brief/239>

36. *June 28, CNET News* — **Gaza hack attack.** Hundreds of Israeli Websites were defaced Wednesday, June 28, allegedly by Moroccan hacker group Team Evil, according to a Haaretz.com post. The Website defacements, whose targets included banks and hospitals, carried the message: "Hacked By Team–Evil Arab hackers u KIll palestin people we Kill Israel servers," according to a posting on Zone–h Internet thermometer Website.

Source: [http://news.com.com/2061–10789\\_3–6089019.html](http://news.com.com/2061–10789_3–6089019.html)

37. *June 28, GovExec* — **Navy contractor arrested for alleged computer system sabotage.** A Navy contractor was arrested Monday, June 26, in connection with planting malicious code on a government computer system. Richard Sylvestre owned and worked for Ares Systems International. SAIC Corp. recently won a contract to provide a third network administrator at the center, the filing said, beating Ares, which also had submitted a bid to fill the position. According to the complaint, two network computers at the center went offline unexpectedly on May 21. Both Ares contractors were away on travel and the SAIC systems administrator found the computers had been programmed with malicious code that deleted critical operating system files. Further investigation revealed similar code on three other computers, including a network server, although that code had not yet executed. Later, investigators used computer records and interviews to trace the malicious code back to Sylvestre.

Source: [http://govexec.com/story\\_page.cfm?articleid=34443&dcn=todays\\_news](http://govexec.com/story_page.cfm?articleid=34443&dcn=todays_news)

**38. *June 28, IDG News Service* — Researcher publishes details of Amazon.com, MSN holes.**

Frustrated with what he calls a lack of response from Microsoft and Amazon.com, a security researcher has gone public with details of flaws on the two companies' Websites. The flaws could be used by attackers to steal "cookie" data files that would allow them to access Amazon.com and MSN accounts, or to display a fake login page that could be used in phishing attacks, according to Yash Kadakia, the independent security researcher who discovered the flaws. Although the cross-site scripting flaws he discovered are generally considered to be low-risk problems, Kadakia's attack involves a technique called Carriage Return Line Feed injection, which can be used in a more serious and widespread attack, he said. Kadakia said he first notified Microsoft of the problem about a year ago. But he said he was not taken seriously until late last week, when he posted screen shots of the flaw being exploited on his Website. The Amazon.com flaw was discovered in December, but after some initial discussions with the Web retailer, the vulnerability remained unpatched, Kadakia said.

Source: <http://www.networkworld.com/news/2006/062906-researcher-publishes-details-of-amazoncom.html>

**39. *June 28, Tech Web* — Two new IE bugs uncovered.** Security analysts Wednesday, June 28, warned users of a pair of unpatched bugs in Microsoft's popular Internet Explorer (IE) browser that may soon be in play because proof-of-concept code has gone public for both. The two vulnerabilities have been detailed on the Full Disclosure security mailing list, and were the root of alerts issued by the SANS Institute's Internet Storm Center and Symantec Corp. on Wednesday. One vulnerability lets attackers execute their code remotely if they can dupe users into double-clicking on a file included in a malicious Webpage. The second flaw is due to a failure of IE to enforce cross-domain policies, Symantec said in a warning to customers of its DeepSight threat system.

Source: <http://www.techweb.com/wire/security/189602387;jsessionid=YWAY1ZXZYRXXI0QSNDLRCKHSCJUNN2JVN>

### **Internet Alert Dashboard**

#### **DHS/US-CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of publicly available exploit code for an unpatched buffer overflow vulnerability in Microsoft Hyperlink Object Library (HLINK.DLL). By persuading a user to access a specially crafted hyperlink in an email message or MS Office document, a remote attacker may be able to execute arbitrary code with the privileges of the user.

More information about this vulnerability can be found in the following:

VU#394444 – Microsoft Hyperlink Object Library stack buffer overflow:  
<http://www.kb.cert.org/vuls/id/394444>

Until an update, patch, or more information becomes available, US-CERT recommends the following:

Do not follow unsolicited web links received in email messages or embedded in MS Office documents.

US-CERT will continue to update current activity as more information becomes available.

## PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

## Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 445 (microsoft-ds), 50497 (----), 6881 (bittorrent), 6623 (----), 26777 (----), 24232 (----), 80 (www), 4672 (eMule), 25 (smtp)
----------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

40. *June 29, Associated Press* — **Peak flow at Maryland's Conowingo Dam may cause flooding.** Cecil County, MD, officials asked residents of about 300 properties in low-lying areas to evacuate Thursday, June 29, before the Susquehanna River reaches peak flow. Exelon Generation, which operates the Conowingo Dam across the Susquehanna, says peak flow from recent heavy rains is expected about 11 p.m. EDT Thursday. Exelon says 22 of the dam's 50 gates are already open and 26 to 28 are expected to be opened. Flooding usually begins at the 22 gate level.

Source: [http://www.wusatv9.com/news/news\\_article.aspx?storyid=50459](http://www.wusatv9.com/news/news_article.aspx?storyid=50459)

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:  
<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.